



Transportation Security Administration

Privacy Impact Assessment for the BWI-PIT Sterile Area Access by Non-Ticketed Individuals

December 9, 2005

Contact Point

Richard Hayes

Director, Infrastructure, Aviation Programs
Transportation Security Administration
(571) 227-3279

Reviewing Officials

Lisa Dean

Privacy Officer

Transportation Security Administration
(571) 227-3947

Maureen Cooney

Acting Chief Privacy Officer

Department of Homeland Security
(571) 227-3813



Introduction

The airport operating authorities at Baltimore-Washington International Thurgood Marshall Airport (BWI) and Pittsburgh International Airport (PIT) seek to establish a program under which non-ticketed individuals may be given access to the sterile area of the airport in order to accompany or meet passengers at a gate, or to shop or dine at concessions located within the sterile area. The sterile area is “a portion of an airport defined in the airport security program that provides passengers access to boarding aircraft and to which the access generally is controlled by TSA, or by an aircraft operator under part 1544 of this chapter or a foreign air carrier under part 1546 of this chapter, through the screening of persons and property.” 49 CFR § 1540.5. The sterile area of the airport may include concession areas such as stores, restaurants, and other facilities which operate beyond the Transportation Security Administration (TSA) security checkpoints. In general, only ticketed passengers with valid boarding passes, airport employees, and airline employees are permitted to gain access to these areas after undergoing required security screening.

TSA has broad authority under 49 U.S.C. §§ 114(l) and 40113(a) to assess threats and threat information and to plan and execute such actions as may be appropriate to address threats to transportation. TSA has determined that implementation of certain security measures is necessary to permit non-ticketed individuals to access the sterile areas of BWI and PIT. In order to implement this program, and in accordance with current protocols applying to air carriers, TSA has issued security directives requiring Airport Operators at PIT and BWI to compare the name and identification¹ of each non-ticketed individual who wishes to access the sterile areas of the airport with that of individuals on the No-Fly and Selectee Lists. Airport Operators may request additional information such as date of birth to resolve any possible matches to these lists.

The No-Fly List and a portion of the Selectee List are maintained by the Terrorist Screening Center (TSC). The TSC maintains responsibility over the Federal Government’s consolidated terrorist watch lists, including the No-Fly and Selectee Lists, in an integrated database known as the Terrorist Screening Database (TSDB). TSA maintains a portion of the Selectee List that includes individuals who pose a threat to transportation security who may not be linked to terrorism. The No-Fly and Selectee List components of the TSDB and the portion of the Selectee List that may be maintained by TSA are the basis for the checks conducted by the Airport Operators. TSA will provide copies of these lists to the BWI and PIT airport operators to carry out the watch list screening function for individuals who wish access to the sterile areas of these airports. If the Airport Operator determines that there may be a match to the watch lists, it will refer the name to TSA for resolution of the possible match and/or for operational response.

Because this program entails a new collection of information about members of the public in an identifiable form, the E-Government Act of 2002 requires that TSA conduct a Privacy Impact Assessment (PIA).

¹ Either of the following forms of identification is required: one form of government-issued photo identification or two other forms of identification, at least one of which must be government-issued.



Section 1.0

Information collected and maintained

1.1 What information is to be collected?

The Airport Operators, not TSA, will collect the non-ticketed individual's name and compare the individual's name and identification against the No-Fly list and the Selectee Lists. In the vast majority of cases, the personal information identified on a government-issued identification will be sufficient to eliminate the possibility that the individual is a person on the No-Fly or Selectee Lists. In the event that the Airport Operator determines that the individual is a positive or suspected match to the No-Fly List, the operator will not issue a checkpoint pass to that individual or to any other individual(s) accompanying the individual. Instead, the Airport Operator will send the individual's name and personally identifying information to the Federal Security Director (FSD) (or designee) and the appropriate Law Enforcement Officer (LEO) and provide the responding LEO with all corresponding identifying data and available identifying information provided by the individual to determine if the individual is a match to the No-Fly List. If the LEO determines that there is not a match, the Airport Operator may issue a checkpoint pass to the non-ticketed individual requesting access to the sterile area. If the LEO determines there is or may be a match, TSA will be notified for resolution and/or possible operational response. In the event that the Airport Operator determines that the individual is a positive or suspected match to the Selectee List, the Operator will notify TSA and issue the individual a checkpoint pass. The individual will be subject to appropriate screening at the screening checkpoint.

Upon TSA request, the Airport Operator may also forward to TSA lists of all non-ticketed individuals who are permitted access to the sterile areas of the airports. These lists will only be requested for audit purposes or to investigate an incident at the airport.

Information collected for the Redress Process

In order to assist in ruling out a possible match to the No-Fly List or Selectee List, the Airport Operator may request additional information directly from the individual. In addition, a redress process will be available to assist individuals who feel that they have been wrongfully denied access to the sterile areas of an airport based on the No-Fly List check conducted by the Airport Operators. The individual may contact the TSA Contact Center at 1-(866)289-9673 or TSA-ContactCenter@dhs.gov for assistance. During the redress process, it may be necessary for TSA to collect additional information from the individual in order to facilitate the redress process, which may include notarized copies of identification documents such as a birth certificate or passport. If TSA needs additional information in order to continue the process, the individual will be notified in writing. The information requested will be the minimum necessary to complete the redress process.

1.2 From whom is information collected?

The Airport Operator, not TSA, will collect the personally identifying data directly from non-ticketed individuals who wish access to the sterile areas of an airport. TSA will only receive the names and personal identifying information of individuals who match or are suspected matches to the No-Fly and Selectee Lists. TSA will also audit the performance of the airport operator by periodically reviewing lists of all individuals admitted to the sterile area under this program.



1.3 Why is the information being collected?

The purpose of collecting this information is to permit non-ticketed individuals access to the sterile areas of the airport to accompany ticketed passengers or to shop at concessions located in these areas while maintaining appropriate security in these areas.

1.4 What specific legal authorities/arrangements/agreements define the collection of information?

Under 49 U.S.C. §§ 114(l) and 40113(a), TSA has broad authority to issue regulations to carry out its statutory functions. TSA has issued the Transportation Security regulations (TSRs), which, among other things, establish security obligations of Airport Operators. Airport Operator security requirements contained at 49 CFR Part 1542 apply to Airport Operators identified at 49 CFR § 1542.1. Pursuant to this authority, TSA is requiring Airport Operators at BWI and PIT to collect and compare the names and personally identifying data of non-traveling individuals who wish access to the sterile areas of the airport against the No-Fly and Selectee Lists.

Privacy Impact Analysis: TSA will only receive the names and personally identifying data of matches or suspected matches to the TSA No-Fly or Selectee Lists. This process is consistent with the current protocols applicable to air carriers. Limiting the information received by TSA serves the agency's operational purposes while minimizing the privacy risks for individuals who use this means for access to the sterile areas of an airport. Because individuals presenting at the airport will be able to provide their additional identifying information, such as date of birth, it is expected that positive matches reported to TSA will be rare.

Section 2.0 Uses of the system and the information

2.1 Describe all the uses of information.

TSA will use the information concerning the non-ticketed individuals who are positive or suspected matches to the No-Fly List and Selectee Lists for the purpose of identifying actual or potential threats to transportation security, including those who seek to test access controls to the sterile area.

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern (Sometimes referred to as data mining)?

No.



2.3 How will the information collected from individuals or derived from the system be checked for accuracy?

Airport Operators will collect information directly from the individual, and transmit the identifying information concerning positive or suspected watch list matches directly to TSA.

Privacy Impact Analysis: Since the personal information is collected directly from the individual in person at the airport, the risk of collecting inaccurate information is minimized. Individuals who feel they have been wrongly identified as a positive match to the watch lists can seek redress through TSA.

Section 3.0 Retention

3.1 What is the retention period for the data in the system?

TSA will retain the data it receives in accordance with record schedules approved by the National Archives and Records Administration (NARA).

3.2 Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

The applicable record retention schedule covering data on positive or suspected watch list matches is pending approval by NARA. TSA Record Schedule 400.6, which covers the retention of lists of individuals obtained for investigative purposes, has been approved by NARA. The applicable record retention schedule for lists of individuals obtained for audit purposes will be submitted to NARA.

Privacy Impact Analysis: Information collected through this program will be maintained in accordance with NARA-approved record retention schedules in furtherance of TSA's mission to ensure the security of the Nation's transportation system.

Section 4.0 Internal sharing and disclosure

4.1 With which internal organizations is the information shared?

The information TSA receives from Airport Operators may be shared within DHS components that have a need to know the information in order to carry out their official duties, including but not limited to law enforcement or intelligence operations. This information will be shared in accordance with the provisions of the Privacy Act, 5 U.S.C. § 552a.



4.2 For each organization, what information is shared and for what purpose?

TSA only receives the identifying information concerning non-ticketed individuals whose information matches or is a suspected match to the No-Fly List or Selectee List in order to resolve possible matches or for operational response. TSA may share that information within DHS for intelligence, counterintelligence, law enforcement or other official purposes related to transportation security in accordance with the provisions of the Privacy Act.

4.3 How is the information transmitted or disclosed?

Depending on the specific situation and need, TSA may transmit this data within DHS only to those who need the information to perform their official duties via a secure data network, secure facsimile or telephonically. This method of transmission may vary according to specific circumstances. The information may also be marked with specific handling requirements and restrictions to further limit distribution.

Privacy Impact Analysis: Information is shared within DHS with those individuals who have demonstrated a need for the information to perform their official duties in accordance with the Privacy Act. Privacy protections include strict access controls, including security credentials, passwords, real-time auditing that tracks access to electronic information, and mandated training for all employees and contractors.

Section 5.0

External sharing and disclosure

5.1 With which external organizations is the information shared?

TSA may share the information it receives with Federal, state, or local law enforcement or intelligence agencies or with the airport operator or other organizations pursuant to the Privacy Act and in accordance with the routine uses identified in the applicable Privacy Act system of records notice (SORN), DHS/TSA 011, Transportation Security Intelligence Service (TSIS) Operations Files. This SORN was last published in the Federal Register on December 10, 2004, and can be found at 69 FR 71828, 71835.

5.2 What information is shared and for what purpose?

It is expected that individually identifying data and watch list status will be shared to communicate the access status with the Airport Operator and to facilitate an operational response.

5.3 How is the information transmitted or disclosed?

Depending on the recipient and the urgency of the request or disclosure, the information may be disclosed telephonically, electronically via a secure data network, or via a secure facsimile.



5.4 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared?

Not applicable. The Privacy Act System of Records Notice described above provides the necessary allowances for sharing of the information.

5.5 How is the shared information secured by the recipient?

TSA requires any external entity receiving this information to handle it in accordance with the Privacy Act and/or any other applicable handling restrictions.

5.6 What type of training is required for users from agencies outside DHS prior to receiving access to the information?

None. However, TSA requires the data to be handled in accordance with the Privacy Act and/or any other applicable handling restrictions and TSA personnel handling the data are required to complete the required TSA Privacy training prior to handling personally identifiable information.

Privacy Impact Analysis: TSA will share this information under the applicable provisions of the SORN and the Privacy Act. By limiting the sharing of this information and by ensuring that recipients properly handle this data, TSA is mitigating any attendant privacy risks.

Section 6.0 Notice

6.1 Was notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice. If notice was not provided, why not?

Because this program is being implemented by BWI and PIT, the respective Airport Operators are responsible for providing notice of the initial collection of information needed to permit sterile area access. If an individual believes that the results of the screening are inaccurate, he or she will be informed of how to pursue redress from TSA. The publication of this PIA and of the SORN for DHS/TSA 011, Transportation Security Intelligence Service (TSIS) Operations Files, also serve to provide public notice of the collection, use and maintenance of this information. The SORN was last published in the Federal Register on December 10, 2004, and can be found at 69 FR 71828, 71835.



6.2 Do individuals have an opportunity and/or right to decline to provide information?

Yes, this process is voluntary. However, the Airport Operator will not grant individuals access to the Sterile Area unless they provide information that enables the Airport Operator to perform the watch list checks.

6.3 Do individuals have the right to consent to particular uses of the information, and if so, how does the individual exercise the right?

In the first instance, as noted above, individuals have the right to decline to provide their names for checking against the lists that the Airport Operator will have. If an individual provides his or her name and a positive match results, all uses of positive or suspected match information by TSA will be consistent with the Privacy Act and the DHS/TSA 011, Transportation Security Intelligence Service (TSIS) Operations Files SORN identified in paragraph 5.1 above.

Privacy Impact Analysis: The limitation on the information received by TSA serves the agency's operational purposes while minimizing the privacy risks for individuals who use this program for access to the sterile areas of the airport. Non-ticketed individuals presenting at the airport for access to the airport's sterile areas will be able to provide any additional identifying information, such as date of birth, to the Airport Operator or LEO if necessary to distinguish the individual from a name on the No-Fly or Selectee lists. Since the individual can contemporaneously provide this information, it is expected that positive matches reported to TSA will be rare.

Section 7.0

Individual Access, Redress and Correction

7.1 What are the procedures which allow individuals to gain access to their own information?

Individuals may request access to their information by submitting a Freedom of Information Act/Privacy Act (FOIA/PA) request to TSA in writing by mail to the following address:

Transportation Security Administration, TSA-20, West Tower
FOIA Division
601 South 12th Street
Arlington, VA 22202-4220

FOIA/PA requests may also be submitted by fax at 571-227-1406 or by filling out the Customer Service Form (URL: <http://www.tsa.gov/public/contactus>). The FOIA/PA request must contain the following information: Full Name, address and telephone number, and email address (optional). Please refer to the TSA FOIA web site (<http://www.tsa.gov/public>). In addition, individuals may amend their records through the redress process as explained in paragraph 7.2 below.



7.2 What are the procedures for correcting erroneous information?

Individuals may request correction of their information in two ways. First, the Airport Operator may request additional information directly from the non-ticketed individual in order to rule out a possible match to the No-Fly List or Selectee List. In addition, a TSA redress process will be available to assist individuals who feel that they have been wrongfully denied access to the sterile areas of an airport based on the No-Fly or Selectee List checks conducted by the Airport Operators. Individuals will be notified of the redress process by signs posted at the kiosk used by individuals seeking access under this program. The individual may contact the TSA Contact Center at 1-866-289-9673 or TSA-ContactCenter@dhs.gov for assistance. During the redress process, it may be necessary for TSA to collect additional information from the individual in order to facilitate the redress process, including notarized copies of identification documents, such as a birth certificate or passport. If TSA needs such additional information in order to continue the process, the individual will be notified in writing. The information requested will be the minimum necessary to complete the redress process.

In addition to the redress process, the individual may also request correction of the records pursuant to the Privacy Act. While the system of records in which actual or potential matches to the watch lists are maintained is subject to certain exemptions under the Privacy Act, TSA may decide to amend these records when appropriate. Such requests should be sent to the address noted in paragraph 7.1 above.

7.3 How are individuals notified of the procedures for correcting their information?

Individuals may contact the TSA Contact Center for assistance as noted in paragraph 7.2. Individuals will be notified of the redress process by signs posted at the kiosk used by individuals seeking access under this program.

7.4 If no redress is provided, are alternatives are available?

A redress process is provided for individuals who believe that they have been wrongfully denied access to the sterile areas of the airport based on the watch list screening process.

Privacy Impact Analysis: Since the Airport Operators will collect information directly from the individual, the risk of collecting inaccurate information is minimized. In addition, individuals may request access to or correction of their personal information pursuant to a redress process and pursuant to the Privacy Act.

Section 8.0

Technical Access and Security

8.1 Which user group(s) will have access to the system?

In order to perform their duties in managing, upgrading, and using the system, system administrators, security administrators, IT specialists, vetting operators and analysts have access to the system. Automated role-based access controls are employed to limit the access of information by different



users based on the need to know. TSA also employs processes to enforce separation of duties to prevent unauthorized disclosure or modification of information. This system is used internally within DHS and provides no public access. No unauthorized users are permitted access to system resources. Strict adherence to access control policies is automatically enforced by the system in coordination with and through oversight by TSA security officers.

8.2 Will contractors to DHS have access to the system? If so, please submit a copy of the contract describing their role to the Privacy Office with this PIA.

Contractors who are hired to perform many of the IT maintenance and security monitoring tasks have access to the system in order to perform their official duties. Strict adherence to access control policies is automatically enforced by the system in coordination with and through oversight by TSA security officers. All contractors performing this work are subjected to Homeland Security Acquisition Regulation (HSAR) requirements for suitability and a background investigation.

8.3 Does the system use “roles” to assign privileges to users of the system?

Role-based access controls are used for controlling access to the system using the policy of Least Privilege, which states that the system will enforce the most restrictive set of rights/privileges or access needed by users based on their roles.

8.4 What procedures are in place to determine which users may access the system and are they documented?

The system is secured against unauthorized use through the use of a layered, defense-in-depth security approach involving procedural and information security safeguards.

All TSA and DHS employees and assigned contractor staff receive DHS-mandatory privacy training on the use and disclosure of personal data. They also receive appropriate security training and have any necessary background investigations and/or security clearances for access to sensitive information or secured facilities based on TSA security policies and procedures.

All government and contractor personnel are vetted and approved access to the facility where the system is housed, issued picture badges with integrated proximity devices imbedded, and given specific access to areas necessary to perform their job function. A Rules of Behavior document provides an overall guidance of how employees are to protect their physical and technical environment and the data that is handled and processed. All new employees are required to read and sign a copy of the Rules of Behavior prior to getting access to the system.

All personnel working/accessing the facility are required to wear a security office issued control badge with picture and name. The badges provide the electronic access control cards used to gain entrance to the secure area for the computer operations room. Badges must be worn and displayed at all times while on the premises.



8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

Employees or contractors are assigned roles for accessing the system based on their function. The Facility Security Officer ensures compliance to policy and manages the activation or deactivation of accounts and privileges as required or when expired. TSA ensures personnel accessing the system have security training commensurate with their duties and responsibilities. All personnel are trained through TSA's Security and Awareness Training Program when they join the organization and periodically thereafter. The status of personnel who have completed the training is reported to TSA on a monthly basis.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

The system is audited annually by the TSA IT Security Office. An audit trail is maintained on the system to track any changes to the data and to track access to the system.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

All government and contractor personnel are required to complete the annual on-line TSA Privacy Training. Compliance with this requirement is audited monthly by the TSA Privacy Officer. In addition, security training is provided regularly, which helps to raise the level of awareness for protecting personal information being processed.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

Information in TSA's record systems is safeguarded in accordance with the Federal Information Security Management Act of 2002 (Pub.L.107-347), which establishes government-wide computer security and training standards for all persons associated with the management and operation of Federal computer systems.

Currently there are two systems that support this program. The first is a system of web boards accessed by the airport operators for purposes of conducting watch list checks. The system of web boards is operating under an Interim Authority to Operate that will expire on February 4, 2006. It is slated for full C&A, however, by January 31, 2006. The other system that supports this program is the TSANet General Support System, which was granted a 12-month Authority to Operate on November 28, 2005.

Privacy Impact Analysis: Data on the system is secured in accordance with applicable Federal standards. Security controls are in place to protect the confidentiality, availability, and integrity of personal data, including role-based access controls that enforce a strict need to know policy. Physical access to the system is strictly controlled with the use of proximity (RFID) badges and biometrics. The system is housed in a controlled computer center within a secure facility. In addition, administrative controls, such as



periodic monitoring of logs and accounts, help to prevent and/or discover unauthorized access. Audit trails are maintained and monitored to track user access and unauthorized access attempts.

Section 9.0 Technology

9.1 Was the system built from the ground up or purchased and installed?

The system is primarily built from Commercial Off the Shelf (COTS) products. System components include COTS hardware and operating systems. This system was provided to TSA from the Department of Transportation upon TSA stand-up.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

Security and privacy requirements were derived based on the sensitivity category of the system, which is considered to be HIGH sensitivity. The high baseline requirements reflect that stringent controls are needed for protecting the confidentiality, availability, and integrity of data of this system. The system is designed to support the high baseline requirements and protects the integrity and privacy of personal information. This system will complete a FIPS 199 to ensure the categorization of the data is accurately and appropriately labeled and secured.

The Airport Operator, not TSA, collects and compares the non-ticketed individual's personal information to the watch lists. TSA only receives information concerning suspected or positive matches. The TSA system is designed to allow for collection of only those data elements necessary to allow TSA to complete its tasks. Additional information is only requested as needed and in the vast majority of cases, a limited initial set of information will be sufficient to eliminate the possibility that the individual is a person on the No-Fly List or the TSA Selectee List.

9.3 What design choices were made to enhance privacy?

In order to support privacy protections, TSA has developed an information technology infrastructure that will protect against inadvertent use of personally identifying information not required by the government. Access to data collected for this program will be strictly controlled; only TSA employees and contractors with proper security credentials and passwords will have permission to use this information. TSA will not transmit or otherwise share this information with entities outside of DHS that are not listed in the routine uses in the TSIS Privacy Act System of Records Notice which was published in the Federal Register. Additionally, the record system will include a real time audit function to track access to electronic information, and any infractions of information security rules will be dealt with quickly and appropriately. All TSA and assigned contractor staff receive TSA-mandated privacy training on the use and disclosure of personal data. The procedures and policies in place are intended to ensure that no unauthorized access to records occurs and that operational safeguards are firmly in place to prevent system abuses.



Transportation Security Administration

Privacy Impact Assessment
Transportation Security Administration
BWI-PIT Sterile Area Access
December 9, 2005
Page 13

Privacy Impact Analysis: These conscious design choices will limit access to the personal information, thereby mitigating any possible privacy risks associated with this program.

Conclusion

TSA is establishing this program to accommodate requests from airport operating authorities to allow non-passengers access to the sterile area for purposes of accompanying passengers to gates or shopping at concessions within the sterile area, while balancing security concerns associated with permitting such access. Privacy impacts associated with this have been minimized by limiting the information provided to TSA to just those individuals who are a possible or actual match to individuals contained on the No-Fly and Selectee Lists. TSA will use this limited information to assist in resolution of possible matches, and to facilitate an operational response to actual matches to the watch lists.

Responsible Official

Richard Hayes
Director, Infrastructure, Aviation Programs
Transportation Security Administration
Arlington, VA 22202
571-227-3279



Transportation Security Administration

Privacy Impact Assessment
Transportation Security Administration
BWI-PIT Sterile Area Access
December 9, 2005
Page 14

Approval Signature Page

_____ December 9, 2005

Lisa S. Dean
Privacy Officer
Transportation Security Administration

_____ December 9, 2005

Maureen Cooney
Acting Chief Privacy Officer
Department of Homeland Security